What Every Employee Needs to Know About ...

Information SECURITY

State of Utah Enterprise Information Security Office

August 2005

Why Every Employee Plays a Key Role in Information Security

Human Factors

Even the newest and best computer technology can be undermined by security lapses—whether accidental or intentional. If your work involves using a computer, choices you make and actions you take can strengthen or harm the State of Utah's ability to protect information security. By understanding and following the information in this brochure, you will contribute to the State of Utah's success in creating and maintaining the safest information security environment possible.

Fast Changing Threats

Today, we're facing a wider variety of computer threats than ever. Spyware, viruses, worms, denial-of-service incidents, system penetration, fraud—they're all out there, every day, and showing up more often. It's our job to limit the risks to the State of Utah's information systems.

One of the most important elements of our defense is awareness. If, when using our systems, you encounter something that is out of the ordinary, something that just doesn't compute, you can help by letting us know about it. As a system user, your suggestions about improving security are important. We encourage you to share them.

Judgment

Employees and managers are accountable for exercising good information security practices in using the State of Utah's information technology. Your good judgment is a key part of helping to keep electronic information secure. These same tools—your desktop or laptop computer, the Internet, and e-mail—are also available to you for limited personal use. The policy governing this use, like any policy, cannot address all of the specific "do's" and "don'ts," but it does provide a basic framework that acknowledges your personal needs in the broader context of the State of Utah's business needs. We're relying on your good judgment to help maintain the right balance. It will protect you, and protect the State of Utah's information systems.

Why Information Security is Essential to the State of Utah

Information security is a business imperative. Trusted information, like people and equipment, is vital to accomplishing our mission and protecting the reputation of the State of Utah.

Information costs time, money, and effort to create, maintain, and deliver. That's a good investment, because it helps us to do our jobs of helping the State of Utah to succeed. When computer assets must be repaired or replaced because of poor security practices, productivity suffers and valuable assets—including labor, materials, and money—must be diverted from other uses.

We also have legal obligations to protect the confidentiality of employee, customer, and citizen information. We can protect the integrity of the State of Utah and those it represents by protecting the security of information. Partnerships are based on trust. We have an opportunity to ensure that trust every day by exercising the best information security practices possible. This can reduce the risks and vulnerabilities to the State of Utah.

Information Security is Everyone's Business

For More Information & Help

Visit the Information Security Web site
www.security.utah.gov

or

E-mail
dsecure@utah.gov

or

Phone ITS Help Desk
801-538-3440

Delivering Trust in a Changing World

Essential Facts for all Employees

About Safe Handling of Information Resources

You should never leave documents containing restricted, personal, or other sensitive information on a printer, copier, fax machine, or other unprotected areas.

You should back-up your work regularly to protect it from loss. Your supervisor or local LAN staff can provide you with more information about back-up procedures at your location.

You should guard your laptop computer at home, in public places, and during travel. This can protect against the inconvenience of loss or theft, as well as the misuse of business information that may be saved on the computer.

About Your Password

Never share your passwords with anyone, and do not write down your passwords.

When you leave your desktop unattended, use an authorized password-protected screensaver, or log off the network.

Make sure your passwords have eight alphanumeric characters. To make your passwords even stronger, it is recommended that they contain at least three of these four kinds of characters: a character that is not a letter or number (for example, &, #, or $), numbers, capital letters, and lower-case letters.

Your passwords should avoid simple English words, dictionary words, proper names, or personal data, such as birthday, address, or telephone number.

About Authorized & Limited Personal Use of Information Technology

The technology that you use at work is primarily for the authorized business of the State of Utah. It's there to help you do your job.

Limited personal use of desktop and laptop computers, e-mail, and the Internet are permitted, but to protect yourself and the State of Utah, you should consult the acceptable use policy, and discuss this use with your supervisor. A clear understanding of the limitations of this privilege can help you avoid unnecessary problems.

The State of Utah monitors your use of its equipment, e-mail, and the Internet. You need to understand that there is no right to privacy when using these tools—either for department-authorized or limited personal use.

You may not install software—including games and screen savers—without authorization from your LAN staff. Improper installation can compromise the system, and some programs may introduce viruses or result in other problems.

About Reporting Incidents

Be on the lookout for irregularities in automated records and report them to your supervisor.

If, when working with your computer, its programs, files, or the Internet, you suspect that an information security incident has occurred, you should report it immediately to the Help Desk.

You should keep the following contact information handy in case you need to report an information security incident:

E-mail: dsecure@utah.gov
Phone: ITS Help Desk: 801-538-3440

About Computer Viruses

If you encounter something out of the ordinary, such as altered data, unusual system performance, or unsuccessful logon attempts, it may indicate the presence of a virus.

If you suspect that your computer has a virus, that your computer's anti-virus software is no longer current, or that the software does not operate properly, contact your Help Desk.

You should be especially wary of viruses on your laptop computer, handheld computer, CDs, or floppy disks. Frequently scan these items for the presence of viruses. Your local LAN staff can assist you with the appropriate procedures.

About E-mail

E-mail can easily and quietly spread viruses and cause other problems to our computer network.

To prevent this, you should not open messages or attachments sent to you by strangers. You should take the same precautions with messages that have suspicious subject lines. In either cases, your best defense is to delete the message without opening it.

A system as large as ours has a great deal of capacity, but it can become strained by forwarding e-mail chain letters, messages that contain possible hoaxes, advertising, jokes, or other non-business messages. This is especially true in the case of non-business messages that contain attachments, audio, and/or video files.